

What is claimed is:

1. A communication network, comprising:

(A) local communication links,

(B) a plurality of separately located central office switching systems interconnected via trunk circuits for selectively providing switched call connections between at least two of the local communication links in response to predetermined control data messages,

(C) a signaling communication system for two-way communications of said control data messages between said central office switching systems, said signaling communication system interconnecting the central office switching systems;

(D) a signaling gateway, separate from the central office switching systems and connected to said signaling communications system, said signaling gateway including an interface connected to a remote communications network and configured to exchange said control data messages between said remote communication network and said signaling communication system, and

(E) a signaling system security monitor, separate from the central office switching systems, said signaling system security configured to evaluate an encrypted portion of said control data messages so as to authenticate corresponding ones of said control messages and, in response, determine if said control data messages are proper.

2. The communications network according to claim 1 wherein said signaling system security monitor comprises a certification agent configured to exchange and maintain encryption key certificates.

3. The communications network according to claim 1 wherein said signaling system security monitor is configured to issue and decrypt digital time stamps.

4. The communications network according to claim 1 wherein said signaling system security monitor comprises a digital certificate issuing authority.

5. The communications network according to claim 1 wherein said signaling system security monitor is configured to selectively communicate said control data messages between said signaling gateway and said signaling communication system in response to said encrypted portions of said control data messages.

6. The communications network according to claim 1 wherein said signaling system security monitor is configured to selectively enable and inhibit said signaling gateway from exchanging said control data messages between said remote communication network and said signaling communication system in response to said encrypted portions of said control data messages.

1 7. The communications network according to claim 1 wherein said signaling system
2 security monitor includes a memory storing states of respective ones of said central office
3 switching systems, said processor additionally responsive to said states for determining
4 if said control messages are proper.

1 8. The communications network according to claim 1 wherein said signaling gateway
2 is configured to convert SS7 type messages to another packet data format.

9. The communications network according to claim 10 wherein the other packet data
format is an Internet Protocol (IP) format.

10. The communications network according to claim 1 wherein said signaling system
security monitor is configured to monitor at least one of (i) a destination point code, (ii)
an originating point code, and (iii) a service indicator.

1 11. The communications network according to claim 1 wherein said signaling system
2 security monitor is configured to monitor at least one of SCCP, ISUP, TCAP, and AIN
3 messages.

1 12. The communications network according to claim 1 wherein said signaling system
2 security monitor is configured to monitor calling and called party address parameters
3 contained in SCCP message portions of said control data messages and determine if said

4 monitor calling and called party address parameters are consistent with an authorized
5 signaling relationship.

1 13. The communications network according to claim 1 wherein said signaling system
2 security monitor is configured to monitor calling and called party address parameters
3 contained in an SCCP message portion of said control data messages.

10963299-011501
14. The communications network according to claim 1 wherein said signaling system
security monitor is configured to monitor origination and designation point codes and
calling and called party address parameters contained in a TCAP message portion of said
control data messages.

15. The communications network according to claim 1 wherein said signaling system
security monitor is configured to monitor origination and destination point codes
parameters contained in a TCAP message portion of said control data messages and
determine if a particular destination point code is authorized to send a particular TCAP
message to a particular destination point code.

1 16. The communications network according to claim 1 wherein said signaling system
2 security monitor includes a memory storing a state of said communications network.

1 17. The communication network according to claim 1 wherein said signaling system

security monitor includes a memory storing permissible states of said communications network and rules for transitioning from each of said permissible states to others of said permissible states.

18. The communications network according to claim 1 wherein said signaling system security monitor includes a memory storing data relating call progress status with respective sets of control messages appropriate to initiate a next action consistent with a particular service.

19. The communications network according to claim 1 wherein said signaling system security monitor includes a memory storing a plurality of message templates.

20. The communications network according to claim 19 wherein said plurality of message templates are associated with a plurality of service providers.

21. The communications network according to claim 20 wherein said signaling system security monitor associates each of said control data messages with a corresponding one of said service providers and selects one of said message templates in response to the corresponding one of said service providers.

22. The communications network according to claim 1 wherein said signaling system security monitor includes a memory storing sets of templates, each of said sets

corresponding to control messages appropriate to particular call progress flow.

23. The communications network according to claim 22 wherein said templates define message formats, parameters and values associated with control message types selected from SCCP, ISUP, TCAP and AIN type messages.

24. The communications network according to claim 22 wherein said signaling system security monitor is configured to select said sets of templates in response to service provider authorization data associated with respective ones of said control data messages.

25. A method of securely interfacing control links of respective communication networks, comprising the steps of:

exchanging control data messages between a remote communication network and a local signaling communication system;

decrypting a certificate portion of said control messages so as to authenticate origination point code information;

selectively communicating, in response to said decrypting step, control data messages between central office switching systems; and

selectively providing switched call connections between at least two of the local communication links in response to predetermined control data messages.

26. The method according to claim 25 further comprising a step of converting a protocol

of said control data messages between a protocol of said remote communication network and a protocol of said local signaling communication system.

27. The method according to claim 26 wherein one of said protocols is an SS7 compliant message protocol.

28. The method according to claim 27 wherein one of said protocols is an Internet Protocol (IP) format.

29. The method according to claim 25 further comprising a step of monitoring of calling and called party address parameters contained in SCCP message portions of said control data messages.

30. The method according to claim 29 wherein said monitoring step includes determining if said calling and called party address parameters are consistent with an authorized signaling relationship.

31. The method according to claim 25 further comprising a step of monitoring origination and designation point codes and calling and called party address parameters contained in a TCAP message portion of said control data messages.

32. The method according to claim 31 wherein said monitoring step includes monitoring

origination and destination point codes parameters contained in a TCAP message portion of said control data messages and determining if a particular destination point code is authorized to send a particular TCAP message to a particular destination point code.

33. The method according to claim 25 further comprising a step of storing a state of said communications network.

34. The method according to claim 25 further comprising a step of storing (i) permissible states of said communications network and (ii) rules for transitioning from each of said permissible states to others of said permissible states.

35. The method according to claim 25 further comprising a step of storing data relating call progress status with respective sets of control messages appropriate to initiate a next action consistent with a particular service.

36. The method according to claim 25 further comprising a step of storing a plurality of message templates.

37. The method according to claim 36 wherein said plurality of message templates are associated with a plurality of service providers.

38. The method according to claim 37 further comprising steps of:

2 associating each of said control data messages with a corresponding one of said service
3 providers; and
4 selecting one of said message templates in response to the corresponding one of said
5 service providers.

09767292-014804